REQUEST FOR QUOTE (RFQ)

Login.Gov Identity Proofing/Verification and Fraud Detection

in support of:
General Services Administration (GSA)/Technology Transformation Service (TTS)

Issued to:
All Eligible Vendors

Under:
Federal Supply Service (FSS) Schedule 70:
General Purpose Commercial Information Technology Equipment, Software, and Services
SIN 132-51: Information Technology Professional Services
NAICS 541111

Issued by:
National Capital Region
Federal Acquisition Service
301 7th and D Streets
Washington DC, 20407

August 30, 2016
NCR AAS Project Number ID11160060

1.1 GENERAL

The work shall be performed in accordance with all Sections of this RFQ. The principal nature of the requirements described in this solicitation is consistent with services performed by industries in the following Schedules and SINs: Schedule 70 General Purpose Commercial Information Technology Equipment, Software, and Services, SIN 132 51 Information Technology Professional Services

1.2 ORDER TYPE

The contractor shall perform the effort required by this Task Order (TO) on a Time and Materials (T&M) basis. The work shall be performed in accordance with all Sections of this TO and the offeror's General Services Administration (GSA) Multiple Award Schedule (MAS), under which the resulting TO will be placed.

1.3 SERVICES AND PRICES/COSTS

The following abbreviations are used in this price schedule:

NTE	Not-to-Exceed
SOO	Statement of Objectives

1.3.1 BASE PERIOD

CLIN	Description	Transactions	Unit Cost by Volume	Total NTE Ceiling
0001	Task 1, Service Requirement in accordance with Section 2.0 in the SOO		$	$

1.4 SECTION 1 - SUPPLIES OR SERVICES AND PRICE/COSTS TABLES

1.4.1 TIME & MATERIAL LABOR

The labor mix specified in the contractor's quote and incorporated into this order are for estimation purposes. The contractor may increase or decrease, with prior written approval of the AAS Contracting Officer's Representative (COR), the number of hours by labor category, within each labor CLIN as needed to effectively manage the project, provided the total funded labor cost and total hours are not exceeded. Any additional labor categories or increases to total hours or increases to ceilings required during performance must be added to the task order by modification.

2.1 BACKGROUND

Login.Gov (formerly Connect.Gov) is a government-wide, cloud-based "Federated Digital Identity Ecosystem" that enables federal agencies to leverage government-provided digital consumer credentials with greater privacy, security and convenience for consumers. The proposed new acquisitions would provide identity service components for integration into the Login.Gov Shared Authentication Platform, which will replace the contracts currently used to operate the Initial Operational Capability (IOC) phase, and establish the Full Operational Capability (FOC) phase of the program. The FOC will enable a greater number of customer agencies to utilize the program without the need of developing, procuring, and managing user identities. Furthermore, they can leverage and meet the guidelines for shared services and benefit from volume pricing and better cost estimations.

In February 2012, the White House established the Federal Cloud Credential Exchange (FCCX), known as Connect.Gov in the IOC phase, to investigate the potential for a common solution for federated identity and credential exchange across government agencies.

The IOC phase, known as Connect.Gov, provides a secure, privacy-enhancing service that conveniently connects people to online government services and applications using an approved digital credential they may already have and trust. Connect.Gov allows an individual to access agency websites and services by signing in with an approved third-party sign-in partner, thereby eliminating the need for consumers to maintain multiple logins for government agencies. GSA manages Connect.Gov and is responsible for the governance structure and business relationships with agencies, industry and credential service providers (CSPs). The United States Postal Service (USPS) serves as the technology manager and is the entity responsible for providing the operating platform for Connect.Gov.

The FAS ITS Cloud Computing Services Program Management Office (CCS PMO) and the Technology Transformation Service (TTS) 18F are working together to move the Program from its IOC phase (Connect.Gov) to the FOC phase (Login.Gov), which will be an enterprise class, cloud-based service that can provide all Government agencies with the ability to provide their users with digital consumer identities. Based on lessons learned from the IOC and a focus on improving agency and consumer usability, 18F is building a Shared Authentication Platform with a modular technical architecture that will consist of different component services which allow for agile and fast modifications to meet agency needs and industry standards.
18 F and CCS PMO are collaborating to define and acquire with this acquisition one of these component services, namely *Identify Proofing/Verification and Fraud Detection*, which will be integrated into the Login.Gov FOC.

2.1.1 PURPOSE

The Login.Gov Program is undergoing significant modifications in direct response to recent laws passed in Congress and executive orders released by the Executive Office of the President instructing federal agencies to protect citizen data in transactions with the Government:

- The Cybersecurity Information Sharing Act (CISA) passed in October 2015;
- The Cybersecurity National Action Plan (CNAP) released in March 2016 by the Executive Office of the President to identity short- and long-term actions to meet CISA; and
- The Implementation Plan Draft released in April 2016 as a plan for action to Executive Order 13681 - Improving the Security of Consumer Financial Transactions.

The acquisition of the following consumer identity service components which will be integrated by 18F into the Login.Gov Shared Authentication Platform via application program interfaces (APIs):

- *Identity Proofing/Verification and Fraud Detection*
  Identity proofing and verification is a service that verifies an individual's identity based on historical life or aggregated transactional information obtained from public and proprietary data sources. Consumer fraud detection service identifies and detects stolen identities and fraud using behavioral algorithms and device intelligence such as reputation, velocity, geolocation, cloaking, and other relational anomalies with real-time transaction analysis.

The high level objective of this task is for the Contractor to provide GSA TTS access to data and services via API in order to proof user identity online and to assist in ongoing identity verification and validation.

2.1.2 AGENCY MISSION
The mission of GSA is to deliver the best value in real estate, acquisition, and technology services to government and the American people.

2.2 SCOPE
To establish Login.gov, GSA TTS is developing a Shared Authentication Platform, into which they will integrate identity service components. The Contractor shall deliver the following component services for the following task: Identity Proofing/Verification & Fraud Detection

The Government reserves the right to increase the volume of each of the services at any time during the effective performance period. Addition of volume identified will only occur after discussions with the Government and a mutually agreed upon task order modification. No work should be completed until the Contractor is in receipt of the signed modification.

2.3 CURRENT INFORMATION TECHNOLOGY (IT)
Vendors providing identify proofing solutions should expect that their services will be accessed via well-documented APIs over HTTPS. Vendors should expect to provide documentation, credentials supporting access to their APIs, instructions for configuration and setup, and timely response to support requests.

2.4 OBJECTIVES
The opportunity selected by the Login.Gov Team is cloud-based, government-wide, federated identity services and support. Presently, each government agency develops and manages its own identity solutions, holding independent contracts with multiple providers and integrating independently with third-party CSPs or proofers.

Since this need for identity services exists within all Federal Agencies, this opportunity was chosen to affect the broadest government-wide savings through aggregation of demand and to provide the greatest impact across government.

The scope of this acquisition for the Login.gov FOC phase is to issue an award to a selected vendor that provides the following identity component service product which will be integrated into the cloud-based hub developed and operated by 18F to underpin the Login.Gov Shared Authentication Platform:

- *Identity Proofing/Verification and Fraud Detection* verifies an individual's identity based on historical life or aggregated transactional information obtained from public and proprietary data sources and identifies and detects stolen identities and fraud using behavioral algorithms and device intelligence.

2.5 TASKS

2.5.1 TASK ONE- SERVICE REQUIREMENTS

- **Identity Proofing/Verification & Fraud Detection**

The objective of this task is for the Contractor to provide GSA TTS access to data and services via application program interface (API) in order to proof user identity online and to assist in ongoing identity verification and validation. GSA TTS seeks data products and capabilities such as:

- Question support based on known Knowledge Based Authentication (KBV, Out of Wallet (OOW) information)
- Verify address of record matches phone of record
- Financial data validation (e.g., checking, savings, loans, credit cards, and utility account data)
- Other methods of identity validation
- Consumer fraud detection service that identifies and detects stolen identities, synthetic and true name fraud etc. using behavioral algorithms, device intelligence such as reputation, velocity, geolocation, cloaking and other relational anomalies with real-time transaction analysis

The Contractor shall outline their approach to meet this objective and provide a technical description with steps of how their system works along with visuals such as data flow, sequence diagram, code examples, high level architecture etc. Ideally the Contractor should provide procedural, cookbook-style documentation and examples of specific sequences, flows and steps.

In addition, the Contractor shall specify their compliance with the following set of requirements using the attached template "IDP Requirements (Attachment A)" and fill out attached Proofing Sources Sheet (Attachment B) with all attributes that are contained within its data sources.

ID	Requirement	Priority
Coverage & Resolution		
1	Identity data sources that include but aren't limited to FCRA and non-FCRA data sources, public records, utility data, employment/ income details provided directly by employers, credit bureau information, phone records, etc.	Must Have
2	Cover 80% of U.S. population for resolution	Nice to have
3	Cover 75% of U.S. population for resolution	Must have
4	Ability to deliver at a minimum, dynamic combinations of the following attributes to resolve an identity to a single record: ● Legal First Name and Last Name ● Middle Name or Initial ● Current Address: (Parsed and Full) ● Date of Birth: (Parsed and Full) ● Social Security Number: (Parsed and Full) ● Phone Number ● Email Address	Must have

5	Other non-traditional data sources such as document verification, video proofing, facial recognition, biometric capture or other emerging technical methods/sources for resolution	Nice to have
6	Access to non-U.S. data sources	Nice to have
Validation		
7	Ability to provide Out of Wallet Support-Online	Must Have
8	Users should only need to enter data once in the proofing flow and should not need to re-enter information unless needed for business reasons	Must Have
9	Ability to provide Knowledge Based Verification Services-Online using both FCRA or non-FCRA data	Must Have
10	Ability to provide Identity Verification via APIs	Must Have
11	Utilize other non-traditional data sources such as document verification, video proofing, facial recognition, biometric capture, device characteristics, geo-location or other emerging technical methods/sources to proof end users	Nice to have
12	Ability to resolve a single record with a true positive and negative result	Must have
13	Ability to calculate and assign a riskiness score to a single record	Must have
14	Ability to return verbose, granular feedback for pass/fail at each step of the proofing process to help improve and tune pass rates. Demonstrated understanding and ability to categorize as statistically relevant ways utilizing standard scientific method practices. Examples are categorizing data as true positive, false positive, true negative, false negative.	Must have
Fraud Detection		
15	Ability to conduct real-time transaction analysis for potentially fraudulent events and both log events and adjust the proofing flow on a transactional basis	Must Have
16	Ability to identify fraudulent activity trends using behavioral algorithms, relational anomalies and other statistical and machine learning techniques	Must Have
17	Ability to identify and detect device previously used in fraudulent activities based on geolocation, other device attributes and profiles	Nice to Have
18	Record and report on input velocity	Must have

19	Ability to identity, flag and recalculate risk score for user identities impacted by data leaks or hacks in other government or commercial systems	Nice to Have
Logging & Reporting		
20	Ability to provide monthly status report as specified	Must Have
21	Ability to provide maintenance schedule detailing any infrastructure, software or data updates and upgrades, duration, impact on Login.Gov, expected downtime etc.	Must Have
22	Log points of failure and provide regular reports on that	Must Have
23	Ability to export all reports and transactional logs in .CSV format	Must Have
User Experience		
24	Identity verification workflow provides consistent system responses including error messages at each step in the process and at a failure point	Nice to Have
25	Support for English language	Must have
26	Support for multiple languages, including Spanish	Nice to have
27	Contractor identity solutions comply with Section 508 Requirements	Must have
28	Support for multiple flows in each environment to support A/B testing	Nice to Have
Other Requirements		
29	Ability to work with GSA TTS to improve the identity proofing process and outcomes	Must Have
30	Ability to provide test environment, pre-built unit tests, and other relevant documentation to help develop and test the service	Must Have
31	Conforms to NIST LOA3 as defined in NIST 800-63-2	Must-have
32	Ability to deliver physical mail for notification purposes.	Nice to Have
General		
33	Ability to provide detailed raw log information regarding system events, transactions, in a standard format (such as .CSV, pipe, line delimited) with standardized delivery to be determined mutually with the Government	Must have

34	Notify GSA TTS of changes to the identity service component, such as changes to the capabilities, service workflows, the API, interface data specifications, and data sources	Must have
35	Maintain test environments to allow for separation of real test data with the ability for the Government to conduct end-to-end testing that are a mirror of production	Must have
36	Maintain a sandbox environment to allow testing technologies under development	Must have
37	Conduct testing with GSA TTS to include: systems integration, performance, security, and user acceptance	Must have
38	Deliver Systems Interface Specifications document following successful integrations to production and update document as needed	Must have
39	Deliver Procedural Setup Guide following successful integrations to production and update guide as needed	Must have
40	Follow a roadmap to update its service based on NIST 800-63-3	Must have

- **Integration & Configuration**

  Contractor shall provide application integration and configuration shall involve support activities during the initial service initiation & integration of the Contractor supplied service. Contractor shall assist GSA TTS staff in implementing an optimal configuration of workflow, thresholds, fraud detection algorithms etc. based on its prior experience and best practices. In addition the Contractor shall provide the testing, tuning and risk leveling of Contractor services to meet GSA TTS business requirements post initial application integration.

- **Ongoing Tuning & Support**

  Once Login.Gov goes live, the Contractor shall participate in periodic reviews of proofing pass/fail rates and other performance metrics, and tuning exercises in order to improve proofing rates. This will involve the analysis of system configuration, reports, creation of recommendations to improve the results and the underlying identity model, actual changes to the system and the Identity model(s) and supporting structure. The reviews and resulting changes will occur at least every 30 days or at the Government's discretion less often.

- **Operations & Maintenance (O&M) Support**

  The Contractor shall provide operations and maintenance activities associated with the on-going support related to the performance of routine, preventive, predictive, scheduled, and unscheduled actions aimed at preventing credential authentication solution failure and increasing efficiency and reliability on a continuous basis. Contractor shall correct errors and bugs/defects identified during operations on a prioritized basis. The priority and urgency of fixes will be determined by GSA TTS and Contractor's QA staff, in accordance with established processes and standards.

The Contractor shall provide support to investigate, assess, and diagnosis reported incidents and technical problems. Contractor shall maintain the operational status of the solution, trace down potential problems, fix defects and work with GSA TTS to maintain operations and throughput. Contractor shall take appropriate remediation actions to expedite the operational recovery and closure of incidents.

The Contractor shall make minor modifications to the solution if changes in shared authentication platform business processes or available hardware necessitate them. In addition, the Contractor shall perform updates to existing user documentation to reflect changes made based on bug fixes, release updates, and system maintenance.

The Contractor shall provide a copy of its Service Level Agreement (SLA).

- **Technical Support Services**

The Contractor shall provide Tier 2, Tier 3 technical support post integration and work with GSA TTS to troubleshoot, fix and resolve any technical issues involving their service in accordance with defined performance requirements.

- **NIST 800-63-3 Draft**

The Contractor shall outline its approach and roadmap that demonstrates its understanding and roadmap items to update its service based on NIST 800-63-3 Draft for IAL 2.

- **Reports (Operations)**

The Contractor shall deliver a Monthly Status Report. These reports must provide accurate, timely, and complete information supporting reporting requirements. The Monthly Status Report must include the following data elements at a minimum:

a. Total and monthly transactions, proofing success/failure rate, causes of error, fraudulent attempts, reproofing rate, demographics and any other data useful for GSA TTS to make informed decisions on tweaking and improving proofing rate and security of Login.Gov platform
b. Performance Statistics associated with meeting the Performance Requirements
c. Identification of any issues impacting the ability of the provided services, accompanied by possible solutions
d. Status on previously identified issues as well as actions taken to mitigate the situation and/or progress made in rectifying the situation
e. The format will be decided during contract kickoff and discussion between Contractor and the Government
f. The report shall be delivered no later than five business days after the end of the month

- **Maintenance Schedule**

In addition to Monthly Status Reports, Contractor shall provide a maintenance schedule. Contractor shall provide direct POCs that GSA TTS can contact with questions or issues regarding the Contractor's services & solution. Contractor shall continuously monitor performance and report any deviation from previous Monthly Status Report or Task Monitoring meetings.

2.5.2 TASK TWO- SECURITY REQUIREMENTS

2.5.2.1 SUBTASK ONE- SYSTEM SECURITY

- The Contractor shall be subject to all applicable federal and agency-specific IT security directives, standards, policies, and reporting requirements.
- The Contractor shall comply with Federal Information Security Management Act (FISMA) associated guidance and directives to include Federal Information Processing Standards (FIPS), NIST Special Publication (SP) 800 series guidelines (available at: http://csrc.nist.gov/), GSA TTS IT security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of Government IT. Compliance references include:
    - Federal Information Security Management Act (FISMA) of 2002; (44 U.S.C. Section 301. Information Security) available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
    - Federal Information Security Modernization Act of 2014; (to amend Chapter 35 of 44 U.S.C.) available at: https://www.congress.gov/113/bills/s2521/BILLS-113s2521es.pdf
    - Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996," available at: https://www.fismacenter.com/clinger%20cohen.pdf
    - Privacy Act of 1974 (5 U.S.C. § 552a)
    - Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004; available at: http://www.idmanagement.gov/
    - OMB Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended; available at: http://www.whitehouse.gov/omb/circulars_a130_a130trans4/
    - OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies." (Available at: http://www.whitehouse.gov/omb/memoranda_2004)
    - OMB Memorandum M-05-24, "Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors"
    - OMB Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors"
    - OMB Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems"
    - FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems"
    - FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems"
    - FIPS PUB 140-2, "Security Requirements for Cryptographic Modules"

- NIST Special Publication 800-18 Revision 1, “Guide for Developing Security Plans for Federal Information Systems”
- NIST Special Publication 800-30 Revision 1, “Guide for Conducting Risk Assessments”
- NIST Special Publication 800-34 Revision 1, “Contingency Planning Guide for Federal Information Systems”
- NIST SP 800-41, Revision 1, “Guidelines on Firewalls and Firewall Policy”
- NIST SP 800-37, Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”
- NIST Special Publication 800-47, “Security Guide for Interconnecting Information Technology Systems”
- NIST Special Publication 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations”
- NIST Special Publication 800-53A, Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans”
- NIST SP 800-61 Revision 2, “Computer Security Incident Handling llGuide”
- NIST Special Publication 800-88 Revision 1, “Guidelines for Media Sanitization”
- NIST Special Publication 800-128, “Guide for Security-Focused Configuration Management of Information Systems”
- NIST Special Publication 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations”
- NIST SP 800-160 “Systems Security Engineering” Draft
- NIST SP 800-63-2 “Electronic Authentication Guideline”

- Despite enhanced security controls and monitoring, incidents may occur that require immediate response from the Contractor. Incidents could include misuse, fraud, misappropriation, espionage, sabotage, and inadvertent or deliberate compromise of the shared authentication platform. The Contractor shall identify proposed plans, communications and protocols for responding to security and privacy incidents in collaboration with the Government. The Contractor shall comply with incident reporting requirements outlined in NIST SP 800-61 and the U.S. Computer Emergency Readiness Team US-CERT.
- Upon termination or expiration of the contract, once all data is provided back to the Federal Government the Contractor shall discard all Government data according to Federal regulations, and must certify no Government data has been retained unless otherwise authorized.
- The Government will retain unrestricted rights to Government data. The data shall be available to the Government upon request within one business day or within the timeframe specified otherwise in the Government’s request, and shall not be used for any other purpose other than that specified herein. The Contractor shall provide requested data at no additional cost to the Government.
- No data related to the work under this contract shall be released by the Contractor

without the consent of the Government in writing. All requests for release must be submitted in writing to the COR/CO.

- The Contractor shall not disclose sensitive or proprietary information pertaining to GSA TTS or any of its operating units, the U.S. Government, industry, business partners, or consumers to any unauthorized persons. The Contractor shall be subject to any and all penalties imposed by law for unlawful disclosure of sensitive information.
- The Contractor shall immediately notify, in writing, GSA TTS upon discovery of any inadvertent or deliberate disclosures of information other than those pursuant to performing the work under the contract. The Contractor shall work with GSA TTS and make available its resources to work with GSA TTS and other entities to resolve this issue.
- The Contractor shall retain any PII consent logs created pursuant to this contract and transfer the logs to GSA TTS at the expiration of the contract.

2.5.2.2 SUBTASK TWO- AUDIT

The Contractor shall allow GSA TTS to conduct operational and security audits to verify the Contractor's compliance with our SLAs and security standards. The audits will be conducted following these guidelines:

- GSA TTS may perform one audit yearly, and may conduct additional audits after a confirmed security breach (one audit per breach). The Contractor shall accommodate assessments by GSA TTS when requested. Unannounced assessments are required to occur within ten business days from initial notification.
- The Contractor shall make a good-faith effort to answer any questions GSA TTS has, and to give access to requested information (under suitable non-disclosure agreements (NDAs), if necessary). The Contractor shall provide up to 40 hours of staff time per audit; any further time is at the Contractor's discretion and may be billed at the Contractor's professional services rate.
- Audits will be conducted remotely; no on-site visits will be required (in either direction).
- Any issues discovered by the audit shall be remediated by the Contractor in a mutually-agreed-upon timeframe.

The Contractor shall provide GSA TTS with any applicable documentation of their security stance and compliance achievements. Examples include:

- Internal security architecture documentation
- Internal security policies and procedure documentation
- Security compliance reports, such as PCI, SOC 2/3, SIG, CSA CSQ, etc.

GSA TTS will use these documents to assist in evaluating the organization's security stance. As such, GSA TTS will give higher weight to those reports produced by independent auditors.

2.5.2.3 SUBTASK THREE- SECURITY OF DATA INCLUDING PERSONALLY IDENTIFIABLE DATA

- A breach is defined as the actual or possible loss of control, unauthorized disclosure, or unauthorized access, whether physical or electronic, of data from the Contractor's

systems that was transmitted as part of the assertion for identity resolution, in any location that is within the control of the Contractor including the underlying identity verification data sources, where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected.

- By acceptance of, or performance on, this contract, the Contractor agrees that in the event of any actual or suspected breach of as defined in paragraph (1) above, the Contractor shall immediately (and in no event later than within one hour of discovery) report the breach to the GSA TTS Contracting Officer (CO) or the Contracting Officer's Representative (COR), the specified contact for the General Services Administration Incident Response Team, and the US Computer Emergency Readiness Team (US CERT) (http://www.us-cert.gov/). If the breach occurs outside of regular business hours and/or neither the CO nor the COR can be reached, Contractor shall call the phone numbers as specified by the CO or the COR and GSA TTS points of contact (POCs) for emergency contacts outside of business hours within one hour of discovery of the breach. Contractor shall also notify the CO and COR as soon as possible during regular business hours.
- In the event of the actual or possible loss of control, unauthorized disclosure, or unauthorized access, whether physical or electronic, in locations controlled by the Contractor, of personal information about End consumers of the Login.Gov service that were not transmitted as part of the assertion for identity resolution, Contractor shall notify GSA TTS at the earliest opportunity during regular business hours.
- Contractor further certifies that it has a security policy in place that contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, breached. Any notification to End consumers as a result of a breach as defined in paragraph (1) above shall be coordinated with GSA TTS. The method and content of any notification by Contractor as a result of a breach as defined in paragraph (1) above will be subject to the approval of GSA TTS. In the event of a breach as defined in paragraph (1) above, Contractor assumes full responsibility for taking corrective action consistent with GSA Data Breach Notification Procedures (http://www.gsa.gov/portal/directive/d0/content/675850).
- Contractor also agrees to cooperate fully with the CO, the GSA TTS Inspector General, and any other authorized Government investigator during any investigation regarding a breach or suspected breach of personally identifiable information as defined in paragraph (1) above. This cooperation includes providing access to documents and systems for a forensic investigation such as systems logs and server images, to determine how or why the breach occurred and how to prevent a similar occurrence in the future. Contractor shall also correct, at its own cost, the system or protocol to prevent any future similar breach.
- The Contractor further certifies that it has a security policy in place that contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, breached. Any notification to End consumers as a result of a breach as defined in paragraph (1) above shall be coordinated with GSA TTS. The method and content of any notification by the Contractor as a result of a breach as defined in paragraph (1) above will be subject to the approval of GSA TTS. In the event of a breach as defined in paragraph (1) above, the Contractor shall assume full responsibility for taking corrective action consistent with GSA Data Breach Notification Procedures (http://www.gsa.gov/portal/directive/d0/content/675850).

2.5.2.4 SUBTASK FOUR- PERSONALLY IDENTIFIABLE INFORMATION NOTIFICATION REQUIREMENT

The Contractor shall have in place procedures and the capability to promptly notify any individual whose PII/Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate by GSA. The method and content of any notification by the Contractor shall be coordinated with, and subject to the prior approval of GSA, based upon a risk-based analysis conducted by GSA in accordance with GSA Privacy incident Handling Guidance and GSA Privacy Incident Standard Operating Procedures. Notification will not proceed unless GSA has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security.

Subject to GSA analysis of the breach and the terms of its instructions to the Contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by GSA. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information. The Contractor agrees to assist in and comply with PII/Sensitive PII incident remediation and/or mitigation efforts and instructions, including those breaches that are not a result of the Contractor or employee actions, but the Contractor is an unintentional recipient of privacy data. Actions may include allowing GSA incident response personnel to have access to computing equipment or storage devices, complying with instructions to remove emails or files from local or network drives, mobile devices (BlackBerry, Smart Phone, iPad, USB thumb drives, etc...). In the event that a PII/Sensitive PII breach occurs as a result of the violation of a term of this contract by the Contractor or its employees, the Contractor shall, as directed by the contracting officer and at no cost to GSA, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 24 months from discovery of the breach. Should GSA elect to provide and/or procure notification or identity protection services in response to a breach, the Contractor shall be responsible for reimbursing GSA for those expenses. To ensure continuity with existing Government identity protection and credit monitoring efforts, the Contractor shall use the identity protection service provider specified by GSA.

3.0 PACKAGING AND MARKING

The contractor shall provide delivery of electronic copies of progress reports and deliverable completion documentation. Electronic copies shall be delivered via email attachment, IT-Solutions Shop (ITSS) or other media by mutual agreement of the parties.

All final reports and deliverable completion documents should be submitted electronically through GSA's electronic task order system (ITSS) at:

ITSS https://web.itss.gsa.gov/login

NOTE: FAILURE TO SUBMIT THE REPORTS/DELIVERABLES IN ITSS WILL RESULT IN REJECTION OF THE REPORT/DELIVERABLE.

3.1 PACKAGING

All reports and deliverables that are in hard copy format, as opposed to electronic format, and that are physically transported through the U.S. mail or private courier services, are to be securely packaged using the contractor’s best practices.

3.2 MARKING

All reports and deliverables that are in hard copy format, as opposed to electronic format, and that are physically transported through the U.S. mail or private courier services, are to be addressed to the individual at the office or floor at the end destination, with the outside package clearly marked to indicate the order number and the recipient’s office telephone number.

4.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this TO shall be performed by the GSA COR within five working days after receipt of deliverable.

4.2 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to requirements by the GSA COR. Inspection will include, if deemed necessary by the Government, validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

4.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the TO, the contractor's quote, and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

For IT development, the final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government are resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government are corrected.

If the draft deliverable is adequate, the Government has the option to accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables must either be incorporated in the succeeding version of the deliverable, or the contractor must demonstrate to the Government's satisfaction why such comments will not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the requirements stated within this TO, the document may be immediately rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the GSA COR.

For IT development, the final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

4.4 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 5 workdays (unless specified otherwise in Section 5) from Government receipt of the draft deliverable. Upon receipt of the Government comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

4.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The GSA CO/COR will provide written notification of acceptance or rejection of all final deliverables within 15 workdays unless specified otherwise in Section 5. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

4.6 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the contractor, within five workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the GSA COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

5.1 PERIOD OF PERFORMANCE

The period of performance for this TO is a seven-month base period.
BASE PERIOD: September 15,2016 to April 14, 2017

5.2 PLACE OF PERFORMANCE

Place of performance is at the contractor facility, address to be provided upon award.

5.3 HOURS OF OPERATIONS

The hours of operation are to be determined by the contractor; however, the contractor is required to be present for a weekly meeting (to be determined after award).

5.4 TASK ORDER SCHEDULE AND MILESTONE DATES

The following schedule of milestones will be used by the COR to monitor timely progress under this TO.

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

The contractor shall deliver the deliverables listed in the following table:

Item #	Title	Description	Delivery Media and Requirements	Delivery Frequency and/or Due Date
1	Test/Sandbox Environment		Online web access	Throughout Period of Performance
2	API Documentation		Email or online web Access	
3	Monthly Status Report		Email	Monthly
4	Maintenance Schedule		Email	As needed
5	Change, Incident and Problem Management	A plan that states the processes, procedures, standards, documentation, controls, and management of all changes on the project and contract	Via email to COR and designated GSA TTS POCs	Within 15 business days after contract award
6	Test Case Documentation	Test data scripts and scenarios necessary to support integration testing	Via email to COR and designated GSA TTS	Within 15 business days after Kick Off Meeting and

			POCs	as required to support integration testing
7	Test Results	Report findings and incidents based on integration testing	Via email to COR and designated GSA TTS POCs	Within 5 days of completing a round of integration testing

5.4.1 PUBLIC-RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA. The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall demonstrate why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider all of the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

5.4.2 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by email and removable electronic media. The following are the required electronic formats unless stated otherwise, whose versions must be compatible with the latest, commonly available version on the market.

a. Text	MS Word
b. Spreadsheets	MS Excel
c. Briefings	MS PowerPoint
d. Drawings	MS Visio
e. Schedules	MS Project

5.6 PLACE(S) OF DELIVERY

Unclassified deliverables or correspondence shall be submitted electronically to the following website location: https://portal.fas.gsa.gov/

Copies of all deliverables shall also be delivered electronically to the TTS/18F Technical POC in a Microsoft format:

To be provided after award:
Telephone: xxx-xxx-xxxx
E-mail: XX

5.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT

The contractor shall notify the GSA COR via a Problem Notification Report (PNR) (Section 9) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

6.1 CONTRACTING OFFICER'S REPRESENTATIVE (GSA COR)

The CO will appoint a COR in writing through a COR Appointment Letter that will be provided to the contractor upon award. The COR will receive, for the Government, all work called for by the Task Order and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to contractor personnel.

The COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the Task Order. Changes will be made only by the CO by properly executed modifications to the Contract or the Task Order.

6.1.1 CONTRACT ADMINISTRATION

Contracting Officer:

Daniel Higgins
GSA FAS AAS
301 7th Street SW
Washington DC, 20407
Telephone: 202-708-5627
Email: Daniel.Higgins@gsa.gov

Contracting Officer's Representative:

TBD
GSA FAS AAS
301 7th and D Streets
Washington DC, 20407
Telephone:
Email:

Technical Point of Contact:

Provided after award.

6.2 INVOICE SUBMISSION

All Requests for Payments by the Contractor shall include the following data elements to be considered for payment:

Task Order Number:	*(from GSA Form 300, Block 2)*
Paying Number:	*(ACT/DAC NO.) (From GSA Form 300, Block 4)*
NCR Project No.:	ID11160060
Project Title*:*	Login.Gov Identity Proofing/Verification and Fraud Detection

The Contractor shall provide invoice backup data, including labor categories, rates, and quantities of labor hours.

A proper invoice shall be submitted monthly and not later than 5 work days after acceptance by the Government of the product, service, and/or cost item. A separate invoice for each task order shall be submitted on official company letterhead with detailed costs for each of the following categories:

1. Total labor charges

2. Travel and per diem charges (if applicable)
3. Total invoice amount
4. Prompt payment discount offered (if applicable)

For other direct costs such as equipment, travel, per diem, subcontractor labor, etc., invoices shall reflect the contractor's actual expense for the item, plus General and Administrative charges (G&A) These charges shall not exceed limits specified in the task order. No charges will be paid by the Government that are not specifically detailed in the individual task order and specifically approved in the underlying contract. Copies of contractor paid invoices, receipts, and travel vouchers completed in accordance with Federal Travel Regulations (FTR) shall be maintained by the contractor and made available to the Government upon request.
In addition to the above information, the invoice shall include the following minimum task identification:

5. GSA Task Order Number
6. Accounting Control Transaction (ACT) number (assigned by GSA on the Delivery Order, GSA Form 300, Block 4)
7. Period of Performance (month services performed for work request task orders, month deliverable completed for fixed price task orders).
8. Invoice Number
9. Client name and address

When the paying office is GSA, the original of each invoice, with supporting documentation, shall be submitted to the GSA Paying Office designated in Block 24 of the GSA Form 300.
In those cases where the paying office is other than GSA, the invoice/paying office will be as specified in the order. One additional copy of each invoice, with supporting documentation, shall be submitted to the address as designated in the order. Invoices for final payment must be so identified and submitted when tasks have been completed and no further charges are to be incurred. These close-out invoices, or a written notification that final invoicing has been completed, must be submitted to the ordering agency within 30 days of task order completion. A copy of the written acceptance of task completion must be attached to final invoices. If the contractor requires an extension of the 30- day period, a request with supporting rationale must be received prior to the end of the 30-day period. Labor hours of subcontractors shall not be billed at a rate other than the fully burdened hourly rates agreed to in the task order or at a rate specifically authorized for the task order as ODC’s.

6.3 INVOICE REQUIREMENTS

Invoices for final payment must be identified and submitted when tasks have been completed and no further charges are to be incurred. The final invoice is desired to be submitted within six months of project completion These are close-out invoices, or a written notification that final invoicing has been completed, must be submitted to the ordering agency within 30 days of task order completion. A copy of the written acceptance of task completion must be attached to final invoices. If the contractor requires an extension of the 30-day period, a request with supporting rationale must be received prior to the end of the 30-day period.

6.3.1 TIME-AND-MATERIAL (T&M) CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the T&M CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section 1 – Supplies or Services and Price/Costs), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following

detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees)
b. Employee company labor category
c. Employee labor category
d. Monthly and total cumulative hours worked
e. Corresponding ceiling rate
f. Cost incurred not billed
g. Current approved forward pricing rate agreement in support of indirect costs billed

7.1 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

7.1.1 ORGANIZATIONAL CONFLICT OF INTEREST

a. Whenever performance of this contract requires access to another Contractor's proprietary information, Contractor shall (i) enter into a written agreement with the other entities involved, as appropriate, in order to protect such proprietary information from unauthorized use or disclosure for as long as it remains proprietary; and (ii) refrain from using such proprietary information other than as agreed to, for example to provide assistance during technical evaluation of other Contractor quotes under this contract. An executed copy of all proprietary information agreements by individual personnel or on a corporate basis shall be furnished to the Contracting Officer within fifteen (15) calendar days of execution.
b. In addition, Contractor shall obtain from each of its employees, whose anticipated responsibility in connection with the work under this contract may be reasonably expected to involve access to such proprietary information, a written agreement, which, in substance, shall provide that such employee shall not, during its employment by the Contractor, or thereafter, improperly disclose such data or information.
c. For breach of any of the above restrictions or for nondisclosure or misrepresentation of any relevant facts required to be disclosed concerning this agreement, the Government reserves the right to pursue all remedies as may be available under law.
d. If in compliance with this clause, the Contractor discovers and promptly reports an organization conflict of interest incident subsequent to this contract, the Contracting Officer may choose to undertake cancellation of the contract.

7.1.2 NON-DISCLOSURE REQUIREMENTS

a. The preliminary and final deliverables and all associated working papers and other material deemed relevant by GSA TTS that have been generated by the Contractor in the performance under this contract are the property of the U.S. Government and must be submitted to the GSA TTS COR at the conclusion of the order.
b. All documents produced for this project are the property of the U.S. Government and cannot be reproduced, or retained by the Contractor. All appropriate project documentation will be given to GSA TTS during and at the end of this contract. Contractor shall not release any information without the written consent of the Contracting Officer. Any request for information relating to the contract presented to Contractor shall be submitted to the Contracting Officer for approval for a response.
c. The Contractor shall not disclose sensitive or proprietary information pertaining to, or in the possession of, GSA TTS or any of its operating units, Government, industry, or business partners or customers to any unauthorized persons. Contractor shall be subject to any and all penalties imposed by law for unlawful disclosure of sensitive information.

7.2 GOVERNMENT FURNISHED PROPERTY (GFP)

The Government will not furnish any property in accordance with performance under this task order. The Contractor shall furnish all facilities, equipment and supplies to ensure successful performance under this task order.

7.3 GOVERNMENT-FURNISHED INFORMATION (GFI)

The Government will not furnish any property in accordance with performance under this task order.

7.4 SECTION 508 COMPLIANCE REQUIREMENTS

Section 508 of the Rehabilitation Act requires Federal agencies to make their electronic and information technology accessible to people with disabilities. This applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. All electronic and information technology (EIT) procured through this task order must meet the applicable accessibility standards specified in 36CFR1194.2, unless an agency exception to this requirement exists. Any agency exceptions applicable to this task order are listed below.

The standards define Electronic and Information Technology, in part, as “any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information. The standards define the type of technology covered and set forth provisions that establish a minimum level of accessibility. The application section of the standards (1194.2) outlines the scope and coverage of the standards. The standards cover the full range of electronic and information technologies in the Federal sector, including those used for communication, duplication, computing, storage, presentation, control, transport and production. This includes computers, software, networks, peripherals and other types of electronic office equipment.

Applicable Standards, which apply to this acquisition

Section 1194.21: Software Applications and Operating Systems _____.
Section 1194.22: Web-based Internet Information and Applications _____X_____.
Section 1194.23: Telecommunications Products _____.
Section 1194.25: Self-Contained, Closed Products _____.
Section 1194.26: Desktop and Portable Computers _____.
Section 1194.31: Functional Performance Criteria _____.

8.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. In addition, all clauses on the master Professional Services Schedule contract apply. Upon request the GSA CO will make their full text available. Also, the full text of any provision is accessible electronically at:

FAR website: https://www.acquisition.gov/far/

Clause No	Clause Title	Date
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.212-4	Contract Terms & Conditions – Commercial Items	MAY 2015
52.219-8	Utilization of Small Business Concerns	OCT 2014
52.227-14	Rights In Data – General Alternate II & III	MAY 2014
52.227-17	Rights In Data Special Works	DEC 2007
52.239-1	Privacy or Security Safeguards	AUG 1996

8.2 FAR CLAUSES IN FULL TEXT

8.2.1 EXERCISE OF OPTION

8.2.1.1 52.217-8 OPTION TO EXTEND SERVICES (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days before expiration.

(End of clause)

8.2.1.2 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days before expiration, provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 30 months.

(End of clause)

8.2.2 52.237-3 CONTINUITY OF SERVICES (JAN 1991)

(a) The Contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The Contractor agrees to --
(1) Furnish phase-in training; and
(2) Exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.
(b) The Contractor shall, upon the Contracting Officer's written notice,
(1) furnish phase-in, phase-out services for up to 90 days after this contract expires and
(2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required.
The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.
(c) The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(End of Clause)

8.2.3 52.224-1 PRIVACY ACT NOTIFICATION (APR 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

(End of clause)

8.2.4 52.224-2 PRIVACY ACT (APR 1984)

(a) The Contractor agrees to -
(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies -
(i) The systems of records; and
(ii) The design, development, or operation work that the contractor is to perform;
(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and
(3) Include this clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.
(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

(c)(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.
(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.
(3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

(End of clause)

8.3 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at:

GSAM website: https://www.acquisition.gov/gsam/gsam.html

Clause No	Clause Title	Date
552.232.25	Prompt Payment	NOV 2009

9.1 LIST OF ATTACHMENTS

Attachment	Title
A	IDP Requirements
B	Proofing Sources Sheet
C	Quality Assurance Surveillance Plan (QASP)
D	Past Performance Questionnaire (To be removed at time of award)
E	Contractor Non-Disclosure Agreement
F	Acronym List

This page is intentionally left blank.

11.1 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the CO will make the full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation of offer. The solicitation provisions and/or contract clauses are available in either HTML or PDF format at:

https://www.acquisition.gov/far

Clause No	Clause Title	Date
52.232-38	Submission of Electronic Funds Transfer Information with Offer	JUL 2013

11.2 GENERAL INSTRUCTIONS

a. The Contractor shall furnish the information required by this solicitation. Contractors shall sign the Standard Form 1449, Block 30. A Standard Form (SF) 1449, "Solicitation/Contract/Order for Commercial Items," completed and signed by the contractor, constitutes the contractor's acceptance of the terms and conditions of the proposed TO. Therefore, the SF 1449 must be executed by a representative of the contractor authorized to commit the contractor to contractual obligations.

b. The Contractor is expected to examine this entire solicitation document including the Contract. Failure to do so will be at the contractor's own risk.

c. The Government may make award based on the initial quote received, without discussion of such quote. Accordingly, the initial quote should be submitted in as complete form as possible and without exception to any provision. The Quote shall set forth full, accurate, and complete information as required by this solicitation package (including Attachments). The penalty for making false statements in quotes is prescribed in 18 U.S.C. § 1001.

d. Contractors submitting restrictive data will mark it as follows in accordance with the FAR 52.215-1, Instructions to Contractors - Competitive Acquisition. Clause 52.215-1 states: "Contractors who include in their quotes data they do not want disclosed to the public for any purpose or used by the Government except for evaluation purposes, shall

Mark the title page with the following legend:

"This quote includes data that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed--in whole or in part--for any purpose other than to evaluate this quote or quotation. If, however, a TO is awarded to this contractor as a result of--or in connection with--the submission of this data, and the Government incorporates the quote as part of the award, the Government shall have the right to duplicate, use, or disclose the data. Also, this restriction does not limit the Government's right to use information contained in

this data if it is obtained from another source without restriction. The data subject to the restriction is contained in sheets (insert numbers or other identification of sheets)"; and

Mark each sheet of data it wishes to restrict with the following legend:

"Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this quote."

e. The Government assumes no liability for disclosure or use of unmarked data and may use or disclose the data for any purpose. Unless restricted, information submitted in response to this request may become subject to disclosure to the public pursuant to the provisions of the Freedom of Information Act (5 U.S.C. § 551).

f. The Government will not pay any Contractor for preparation of their submission.

g. The Vendor must submit their response by the date and time specified on the Standard Form 1449. Late responses will be rejected and not considered for award.

11.3 SUBMISSION OF QUESTIONS

The offeror is requested to submit its questions grouped by solicitation section and make reference to the particular Section/Subsection number. Questions must be received before the date specified for receipt of questions. **Questions or requests for extension submitted after the cut-off date will not be considered**. Any questions regarding this solicitation shall be submitted no later than September 6, 2016 at 2:00 PM Eastern Standard Time via email to Jasmine Mitchell at Jasmine.Mitchell@gsa.gov. The information in response to questions concerning this solicitation will be furnished to the offeror as an amendment to the solicitation.

11.4 SUBMISSION OF QUOTE

All quotes shall be submitted via email to Jasmine.Mitchell@gsa.gov. All responses to the solicitation shall be received by 3:00 PM EST on Thursday, September 8, 2016. Each offer shall be in two parts.

Part I is the written Price Quote and shall contain the following:

a. Solicitation, Offer and Award (SF 1449 (TAB A)
b. Supplies or Services and Prices (TAB B)
c. Price Supporting Documentation (TAB C)
d. Organizational Conflict of Interest Statement (TAB D)
e. Contract Registration (TAB E)

Part II is the written Technical Quote and shall contain the following:

a. Section 508 Compliance Statement (Pass/Fail) (TAB A)
b. Quality Control Plan (QCP) (TAB B)
c. Quality Assurance Surveillance Plan (QASP) (TAB C)
d. Technical Approach (TAB D)
e. Past Performance (TAB E)

NOTE: The technical quote must not exceed 20 double-sided sheets of paper inclusive of text and graphics. Text must be in a font equivalent to Times New Roman, Font 12, or larger.

NOTE: One double-sided sheet of paper is equivalent to 2 single-sided sheets of paper of printed material.

The technical quote shall not contain any pricing information whatsoever.

11.5 SUBMISSION OF THE WRITTEN PRICE QUOTE

The Written Price Quote shall be submitted via email as prescribed above in Section 11.4. The offeror shall submit all proposed prices using PDF, Microsoft Word or Excel software utilizing the formats without cells locked and include all formulas. The quote shall contain the following tabs:

a. Solicitation/Contract/Order for Commercial Items (SF 1449) (Tab A). When completed and signed by the Vendor constitutes the Vendor's acceptance of the terms and conditions of the proposed Task Order. Therefore, the form must be executed by representatives of the Vendor authorized to commit the Vendor to contractual obligations. Vendors shall sign the SF 1449 in Block #30.

b. Supplies or Services and Prices/Costs (Tab B). The offeror shall indicate the price to be charged for each item - Supplies or Services and Price/Costs rounded to the nearest whole dollar.

c. Price Supporting Documentation (Tab C). The information requested in the quote is required to enable the Government to perform a price analysis. The contractor shall prepare one summary schedule which provides the total NTE amount for each CLIN and the total NTE price offered. Along with the summary schedule, the contractor is required to detail the labor categories to be used, labor hours proposed by category, The contractor shall also identify the discounts offered by the contractor and/or the contractor's teaming partners(s).

d. Organizational Conflict of Interest Statement (Tab D). The offeror shall complete and sign an OCI Statement in which the offeror (and any subcontractors, consultants, or teaming partners) disclose information concerning actual or potential OCI affecting the offeror's quote or any work related to this RFQ. The statement should be accompanied by the offeror's plan for mitigation, avoidance, or neutralization, if appropriate.

e. Contract Registration (Tab E). The offeror shall submit a statement that the contract vehicle under which this quote is being submitted has been registered in ITSS (https://portal.fas.gsa.gov).

11.5.1 SUBMISSION OF THE WRITTEN TECHNICAL QUOTE

The offeror shall submit all information described in the following paragraphs. The offeror shall provide an electronic copy containing all required sections of this Part. The written technical shall be **limited to 20 pages, not including the Past Performance Questionnaires (PPQ's)**.

11.5.1.1 SECTION 508 COMPLIANCE REQUIREMENTS (Pass/Fail): (TAB A)

The offeror's written quote shall include a statement indicating its capability to comply with Section 508 requirements throughout its performance of this TO. The offeror's quote will be evaluated to determine whether it includes a statement indicating its capability to comply with Section 508 requirements throughout its performance of this TO. Any quote that does not include a statement indicating the

offeror's capability to comply with Section 508 requirements throughout its performance of this TO shall be eliminated from further consideration for award.

11.5.1.2 QUALITY CONTROL PLAN (QCP) (TAB B)

The offeror shall identify its approach to ensure quality control in meeting the requirements of the Task Order. The offeror shall describe its quality assurance methodology.

11.5.1.3 QUALITY ASSURANCE SURVEILLANCE PLAN (QASP) (TAB C)

Based on the QASP provided by the Government, the offeror shall provide any recommended revisions based on the solution proposed.

11.5.1.4 TECHNICAL APPROACH (TAB D)

The Technical Approach must demonstrate a thorough understanding of Identity Proofing/Verification & Fraud Detection and the requirements of the SOO and describe an approach that will demonstrate the achievement of timely and acceptable performance. The approach must present a proposed Solution to meet the objectives as listed in the SOO.

Specifically, the proposal MUST demonstrate how the offeror will meet the specific tasks in the SOO, including (items are NOT in any order of importance):

- What level of support do you offer to agency customers?
- Data sources and quality.
- Experience working with large systems (1M+ active users)? Be specific as possible.
- How do you detect, prevent and/or handle fraud, identity theft and incidents?
- What overall process flow would you recommend for handling identification, investigation, and remediation to mitigate fraud? How would your fraud detection and prevention algorithms change as a result of the output of that process?
- Describe your lifecycle of previously proofed individuals
- How would you resolve data conflicts and deduping?
- Deliverability metrics
- Disaster Recovery including Mean Time to Recovery (MTTR)
- Demographic coverage of the United States including income level, zip code, age
- Describe past use cases and how you proofed individuals at LOA 3 as defined in NIST 800-63-2

Sub-Factor 1: Requirements Compliance & Proofing Sources
Must fully comply with all "Must have" Requirements shown in the SOO. Compliance with "Nice to have" requirements is not required however it will be favorably rated. In addition, Offeror shall fill out the attached Proofing Sources sheet to specify coverage of data attributes. *See Attachment - Requirements Compliance & Proofing Sources spreadsheet.*

Sub-Factor 2: Product/Service Roadmap (Past and Future)
How do you plan to improve on your service offering in next 12 months and over 3 years?

Sub-Factor 3: Service Level Agreement
To what extent does offeror's Service Level Agreement (SLA) meet or exceed the specified performance metrics and terms addressing Offeror's failure to meet them.

Sub-Factor 4: Security Compliance
Offerors shall provide a copy of their existing security compliance audit reports/certificates (ISO, PCI, SOC II, SOC III etc.) and/or other material that demonstrates their adherence to high security standards.

The Technical Approach will be evaluated based on successful demonstration of the items listed above.

11.5.1.5 PAST PERFORMANCE (TAB E)

Past Performance will be used to make a determination of the extent that the Contractor has more than a satisfactory record of past performance history in similar contracts or task orders working as the prime Contractor on at least five similar contracts in the past 5 years prior to issuance of this solicitation. Past Performance can be either commercial and/or government references.

"Similar Contracts/Task Orders" means providing any support services for Identity Proofing/Verification & Fraud Detection which include Factor 1 and any of the Sub-Factors.

Submission of three Past Performance Questionnaires (PPQ's) is required. As stated earlier, failure to comply with the terms and conditions of this RFP or failure to submit ALL documents required may result in the Proposal being removed from consideration for award of the Task Order.

The PPQ should be completed by a person or reference with direct knowledge of the Contractor and Contract/Task Order referenced. One PPQ should be completed for each requirement for which experience is being claimed. After completion of the PPQ, the person or reference that completed the PPQ shall email the form to kirsten.green@gsa.gov; either Word or PDF formats are acceptable. PPQ's submitted by the Contractor named on the PPQ will not be considered for evaluation. The PPQ should be filled out in its entirety, incomplete PPQ's will not be considered for evaluation. It is the Contractor named on the PPQ responsibility to ensure the person or reference understands all of the facts listed above.

The PPQ's are considered separate documents and shall not to be included as part of the 20 page limitation to the technical proposal. See attachment PPQ for the actual questionnaire and submission details.

In addition to reviewing the PPQ's, the Government may utilize any electronic database or source available to check past performance and any other reference information it obtains on its own.

12.1 METHOD OF AWARD

The Government anticipates awarding a TO to the offeror whose quote is the most advantageous to the Government, price and other factors considered. Technical quotes will be evaluated based on the factors described in Section 12.4. All evaluation factors other than price, when combined, are (significantly more important than price, significantly less important than price, or approximately equal to price.) Award will be made to the offeror whose quote is determined be the best value for the Government.

Quotes shall set forth full, accurate, and complete information as required by this solicitation package (including Attachments). The penalty for making false statements in quotes is prescribed in 18 U.S.C. 1001.

12.2 EXPLANANTION FOR BASIS OF AWARD

This award will be made under FAR 8.4; formal debriefings will not be conducted. In accordance with 8.405-2(d), a brief explanation of the basis for the award decision shall be provided upon request.

12. 3 PRICE EVALUATION

The offeror's written price quote will be evaluated by the Government for price reasonableness. The Government will reject any quote that includes any assumptions to the requirements herein. Tab D will be evaluated to assess whether or not an actual or potential Organizational Conflict of Interest exists. If a disclosed conflict of interest is found to exist that cannot be mitigated, avoided, or waived in accordance with FAR Part 9.5, that offeror will be ineligible for award.

The Government will evaluate each price quote for reasonableness of its pricing. The Government will consider the level of effort and the mix of labor proposed to perform a specific task being ordered, and for determining that the total price is reasonable.

In accordance with FAR 52.217-5, Evaluation of Options the Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. Additionally, in accordance with GSA PIN 2015-01, to determine a total evaluated price, the Government will take the price for all CLINs of the task order, determine a six-month value, and add the value to the sum of the base period. Offerors shall not submit a price for the potential six-month extension of services.

12.3.1 ORGANIZATIONAL CONFLICT OF INTEREST

Tab D will be evaluated to assess whether or not an actual or potential OCI exists as defined by FAR Part 9.5. If an actual or potential conflict of interest is identified that cannot be feasibly mitigated, avoided, or resolved in accordance with FAR Part 9.5, the offeror may be ineligible for award.

12.3.2 PRICE ASSUMPTIONS

The Government reserves the right to reject any proposal that includes any price assumptions that may adversely impact satisfying the Government's requirements.

12.3.3 OVERTIME AND EXTENDED BILLING HOUR PRACTICES

The Government reserves the right to reject any proposal that includes overtime or extended hours billing practices that adversely impact or affect the Government's requirements.

12.4 TECHNICAL EVALUATION FACTORS

The Government will evaluate technical quotes for technical acceptability based on the following:

Non-Price Factors
Factor 1 – Technical Approach
Factor 2 – Past Performance

The technical quote will be evaluated to determine that it meets the Government's requirements as described in the Statement of Objectives. The technical quote will be evaluated as Acceptable/Not Acceptable. A Not Acceptable on any single criteria will make the quote ineligible for award, with no further evaluation of the technical and pricing quote accomplished by the Government.

12.4.1 FACTOR 1: TECHNICAL APPROACH

The Technical Approach must demonstrate a thorough understanding of Identity Proofing/Verification & Fraud Detection and the requirements of the SOO and describe an approach that will demonstrate the achievement of timely and acceptable performance. The approach must present a proposed Solution to meet the objectives as listed in the SOO.

Specifically, the proposal MUST demonstrate how the offeror will meet the specific tasks in the SOO, including (items are NOT in any order of importance):

- What level of support do you offer to agency customers?
- Data sources and quality.
- Experience working with large systems (1M+ active users)? Be specific as possible.
- How do you detect, prevent and/or handle fraud, identity theft and incidents?
- What overall process flow would you recommend for handling identification, investigation, and remediation to mitigate fraud? How would your fraud detection and prevention algorithms change as a result of the output of that process?
- Describe your lifecycle of previously proofed individuals
- How would you resolve data conflicts and deduping?
- Deliverability metrics
- Disaster Recovery including Mean Time to Recovery (MTTR)
- Demographic coverage of the United States including income level, zip code, age
- Describe past use cases and how you proofed individuals at LOA 3 as defined in NIST 800-63-2

Sub-Factor 1: Requirements Compliance & Proofing Sources
Must fully comply with all "Must have" Requirements shown in the SOO. Compliance with "Nice to have" requirements is not required however it will be favorably rated. In addition, Offeror shall fill out the attached Proofing Sources sheet to specify coverage of data attributes. *See Attachment - Requirements Compliance & Proofing Sources spreadsheet.*

Sub-Factor 2: Product/Service Roadmap (Past and Future)
How do you plan to improve on your service offering in next 12 months and over 3 years?

Sub-Factor 3: Service Level Agreement

To what extent does offeror's Service Level Agreement (SLA) meet or exceed the specified performance metrics and terms addressing Offeror's failure to meet them.

Sub-Factor 4: Security Compliance
Offerors shall provide a copy of their existing security compliance audit reports/certificates (ISO, PCI, SOC II, SOC III etc.) and/or other material that demonstrates their adherence to high security standards.

The Technical Approach will be evaluated based on successful demonstration of the items listed above.

12.4.1 FACTOR 2: PAST PERFORMANCE

Past Performance will be used to make a determination of the extent that the Contractor has more than a satisfactory record of past performance history in similar contracts or task orders working as the prime Contractor on at least five similar contracts in the past 5 years prior to issuance of this solicitation. Past Performance can be either commercial and/or government references.

"Similar Contracts/Task Orders" means providing any support services for Identity Proofing/Verification & Fraud Detection which include Factor 1 and any of the Sub-Factors.

Submission of three Past Performance Questionnaires (PPQ's) is required. As stated earlier, failure to comply with the terms and conditions of this RFP or failure to submit ALL documents required may result in the Proposal being removed from consideration for award of the Task Order.

The PPQ should be completed by a person or reference with direct knowledge of the Contractor and Contract/Task Order referenced. One PPQ should be completed for each requirement for which experience is being claimed. After completion of the PPQ, the person or reference that completed the PPQ shall email the form to kirsten.green@gsa.gov; either Word or PDF formats are acceptable. PPQ's submitted by the Contractor named on the PPQ will not be considered for evaluation. The PPQ should be filled out in its entirety, incomplete PPQ's will not be considered for evaluation. It is the Contractor named on the PPQ responsibility to ensure the person or reference understands all of the facts listed above.

The PPQ's are considered separate documents and shall not to be included as part of the 20 page limitation to the technical proposal. See attachment PPQ for the actual questionnaire and submission details.

In addition to reviewing the PPQ's, the Government may utilize any electronic database or source available to check past performance and any other reference information it obtains on its own.

12.5 TECHNICAL ASSUMPTIONS

Offeror assumptions will be reviewed in the context of the technical factor to which they apply. The Government reserves the right to reject any quote that includes any assumption that may adversely impact satisfying the Government's requirements.